Appendix A. RFC 2002 - Mobile IP.

This section briefly describes standard Mobile IP (RFC 2002) and issues related to Mobile IP.

Mobile IP Overview.

Mobile IP has 3 primary software components: a) at least 1 home agent for each "home" IP subnet, b) foreign agents on remote IP subnets, and c) mobile hosts. In addition, a non-mobile host can also contain a Mobile IP software component that processes mobile host "redirect" messages to avoid "triangular routing". [In this discussion, it is assumed that the underlying network is Ethernet; however, the concepts apply to other networking environments.]

A Mobile IP foreign agent entity can exist in a node located on the infrastructure (i.e. in an AP) and/or it can exist in the mobile host. Mobile IP agents that are located on the infrastructure send periodic agent "advertisements" to a multicast IP address, and a corresponding multicast Ethernet address. An agent advertisement is actually a standard ICMP router advertisement packet that also contains Mobile IP optional parameters. A node can detect that it has roamed to a "foreign" subnet, for example, when it receives an agent advertisement from a foreign agent on the foreign subnet. The foreign agent provides a single "care-of" IP address for the foreign subnet for client mobile hosts. The foreign agent must be capable of serving as the default router for client mobile hosts.

If the foreign agent entity is contained in the mobile host, then the mobile host must obtain a care-of address, default router address, and subnet mask from some external means, such as DHCP, when it roams to a foreign subnet. The standard does not indicate how roaming detection is accomplished if the foreign agent entity is contained in the mobile host.

The care-of IP address for a mobile host on a foreign subnet is registered with the home agent The home agent receives IP packets, transmitted on the home subnet, which are destined to the mobile host The packets are encapsulated and forwarded to the current care-of address of the mobile host In an Ethernet environment, the home agent transmits several "gratuitous ARP" packets, when a mobile host first roams to a foreign subnet, which contain the target and source IP address of the mobile host and the source Ethernet address of the home agent interface. The gratuitous ARP packets cause hosts on the home subnet to update any respective ARP cache entry for the mobile host and send packets, destined to the IP address of the mobile host, to the Ethernet address of the home agent. If the home agent receives an ARP request, directed to the IP address of a registered mobile host on a foreign subnet, it will send a "proxy ARP" reply packet with the source Ethernet address of the home agent interface.

Both the mobile host and the home agent transmit several gratuitous ARP packets when a mobile host first returns to its home subnet. In this case, the gratuitous ARP packets contain the target and source IP address of the mobile host and the source Ethernet address of the mobile host. The gratuitous ARP packets cause hosts on the home subnet to update their respective ARP cache entry for the mobile host and send packets directly to the Ethernet address of the mobile host.

Mobile IP Issues.

Several issues, related to the standard Mobile IP protocol, described below.

A mobile host must contain a "special" TCP/IP protocol stack that supports Mobile IP [Note that most personal computers are packaged with a TCP/IP stack that does not support Mobile IP] In most cases, Mobile IP software cannot operate as a UDP application on top of an existing IP stack, for several reasons: a) Application software cannot receive Mobile IP agent advertisements contained in ICMP router advertisement packets; b) application software cannot generate an agent solicitation contained in an ICMP router solicitation packet; c) application software cannot select the destination MAC address for an IP packet, and d) application software cannot inhibit ARP requests. [The Mobile IP specification prohibits the

transmission of ARP Request packets when a mobile host is attached to a foreign subnet.] The problem can be solved by embedding a "proxy Mobile IP client" entity in the data link layer in a mobile host.

If foreign agent entities are contained in mobile hosts, then a proprietary data link subnet roaming detection mechanism must be used. The data link layer and network layer, in a mobile host, must agree on a proprietary interface for subnet roaming indications. The foreign agent entity in the mobile host must use an external mechanism, such as DHCP or BOOTP, to obtain a guest IP address, a new subnet mask, and a new default router address. In most cases, extra IP addresses must be reserved, on each foreign subnet, for roaming hosts.

If foreign agent entities exist in devices on the infrastructure, then foreign agent advertisements can be used for roaming detection. If the mobile host does not support data link roaming indications, then foreign agent advertisements must occur fairly rapidly to facilitate fast roaming; however, RFC 1256 requires a minimum interval of 3 seconds between router advertisements. [If the mobile host supports (i.e. proprietary) data link roaming indications, then the mobile host can send an "Agent Solicitation" packet whenever it roams to a new AP on the same subnet or another subnet. Note that a "roaming indication" is not the same as a "subnet roaming indication".] When a mobile host roams to a foreign subnet, any messages which are sent to the mobile host will be lost until the station receives a foreign agent advertisement, on the foreign subnet, and (re)registers its new care-of address with the home agent. Power-managed mobile hosts will constantly receive the advertisements. As a result, power-managed IP mobile hosts will never sleep. The multicast advertisements consume network bandwidth, which may be significant on a radio link In an 802.11 environment, multicast traffic can delay real-time traffic.

The gratuitous-ARP mechanism, discussed above, is not reliable. For example, if a mobile host roams to a foreign subnet it will register its new care-of address with the home agent that causes the home agent to broadcast several (i.e 3) gratuitous ARP packets. Any host, actively communicating with the mobile host, which misses the broadcast gratuitous ARP packets will continue to send frames to the Ethernet address of the mobile node, therefore those frames will be lost. Note that if a mobile host is roaming rapidly. the gratuitous ARP mechanism will be used repeatedly

Mobile IP may not be transparent to non-mobile hosts because the gratuitous ARP mechanism is based on the assumption that a (i.e. non-mobile) host will update its ARP cache, whenever it receives an ARP packet, even if the target IP address does not belong to the host. [At least one widely used IP implementation discards ARP packets unless the target IP address belongs to the local IP stack.]

The "gratuitous ARP" problem can be solved by assigning each mobile host with an IP address for a home subnet that does not provide access for mobile hosts Since mobile hosts cannot directly attach to the home subnet, traffic for mobile hosts is forced through the IP router for the subnet

Mobile IP only supports IP subnet mobility for IP hosts that are communicating exclusively with the Internet Protocol (IP) A host that is using both IP and IPX, for example, cannot roam to a foreign subnet (i e connected to the home subnet through a multi-protocol router).

Mobile IP creates several security issues A network monitoring tool may "sniff" ARP reply packets and trigger an alarm if more than one hardware address is associated with a single IP address An alarm may also be triggered if the source hardware address in an ARP reply packet is different than the source address of the associated MAC-level frame. The alarms are intended to discover an attacker that is redirecting IP traffic to its MAC address. Note that a Mobile IP proxy ARP packet would trigger such alarms.

Some IP firewalls may prevent Mobile IP from operating. For example, a firewall in a border IP gateway may discard an IP packet if it is received on an interface and the source IP address is not in the domain of the interface. [Such a filter is intended to discard IP packets with fictitious source addresses] Note that the source IP address in an IP packet from a mobile host is the permanent IP address of the mobile host, which is in the domain of the home subnet. Therefore, IP packets from a mobile host may not pass through such a firewall when the mobile host is on a foreign subnet. [The firewall problem can be circumvented by "reverse tunneling", where inbound IP packets from a mobile host on a foreign subnet are also encapsulated

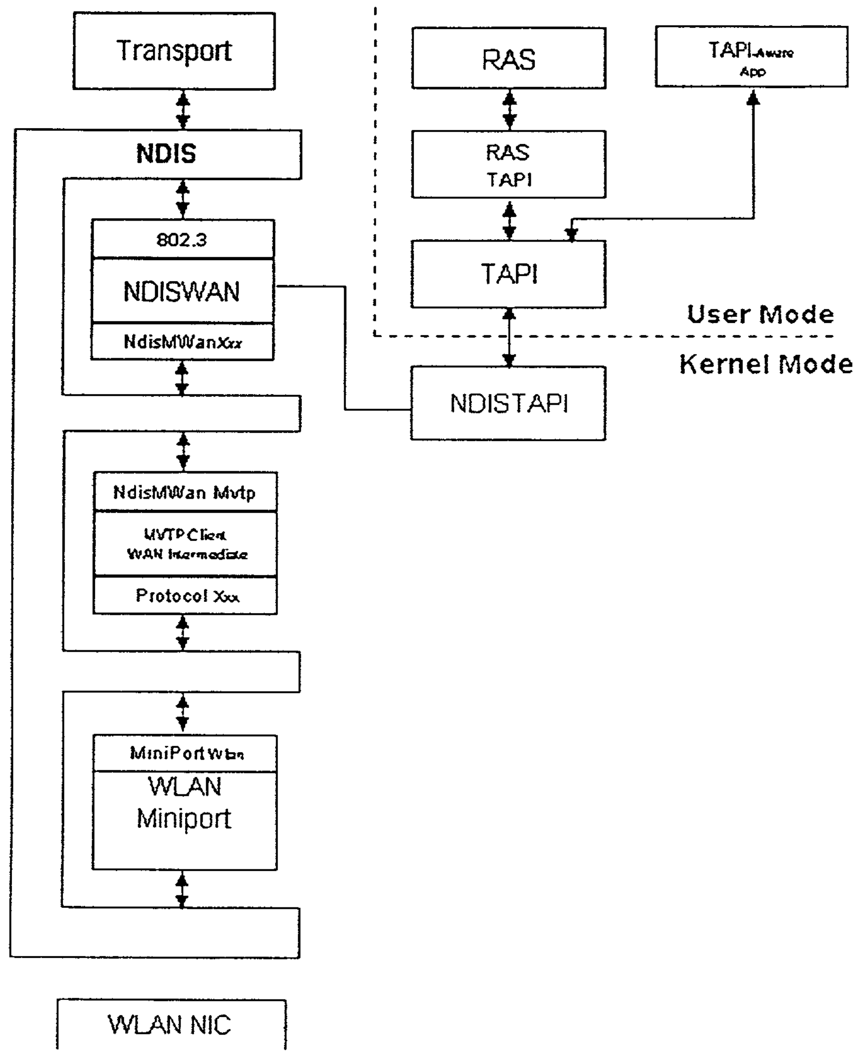
with the current "care-of" address as the source IP address. "Reverse tunneling" is not part of the current Mobile IP standard (RFC 2002). Note that OWL/IP always uses reverse tunneling; therefore, the firewall problem is not an issue for mobile hosts attached through an OWL/IP tunnel.

A Comparison of Mobile VPNP and Mobile IP.

- Both Mobile IP and Mobile VPNP enable a mobile host to access its home network from any location through an IP internetwork. In practice, Mobile IP packets enter the home network through a "firewall". Mobile VPNP packets enter the home network through a point-to-point port on a network access server. Therefore, the firewall problems associated with Mobile IP do not exist for Mobile VPNP.
- Foreign agent detection and subnet roaming detection issues are identical for Mobile IP and Mobile VPNP.
- Mobile IP only supports IP hosts. A global host ID must be an IP address. Mobile VPNP supports any network layer protocol because MVTP provides a general purpose tunneling mechanism that is independent of any higher layer protocol. An MVTP Global Endpoint ID can be any globally unique identifier. Network addresses are dynamically bound to NAS point-to-point subnets with PPP.
- The Mobile IP problems associated with gratuitous ARPs and proxy ARPs do not exist for Mobile VPNP because mobile hosts exist on logical point-to-point links.
- A Mobile VPNP host that is attached to a foreign subnet can obtain a temporary network address, for its home subnet, via PPP NCP. Mobile IP does not support IP broadcast well; therefore it is difficult for a host, attached to a foreign network, to use DHCP and or BOOTP to obtain a temporary home IP address. Also, Mobile IP mobility bindings require a permanent home IP address in the mobile host Mobile VPNP mobility bindings do not require any permanent network address.

Appendix B. Microsoft Windows Mobile PPP Architecture

The relationship among the components that are described in this section is shown in the following diagram.



MVTP uses virtual devices called Mobile Virtual Private Networks (MVPNs). When you configure MVTP, you install and configure MVPNs in RAS as if they were physical devices, just like modems.

Transport Protocols

An IP datagram, IPX datagram, or NetBEUI frame is submitted by its appropriate protocol to the virtual interface that represents the MVPN connection using NDIS. NDIS submits the packet to NDISWAN.

NDISWAN

NDISWAN is an intermediate NDIS driver that provides an IEEE 802.3 miniport interface to protocol drivers and a protocol interface to WAN miniport drivers. NDISWAN provides framing, compression, and encryption services for remote access connections. NDISWAN has a private interface to the kernel-mode NDISTAPI driver for dynamically setting up and tearing down TAPI links.

MVTP Client

The MVTP Client is a WAN miniport driver. WAN miniport drivers are NDIS miniport drivers that contain the necessary code to operate dial-up equipment to establish a point to point connection. In this case, MVTP uses a signaling protocol to establish a MVTP connection between a PPP host and an MVTP FA gateway. Also, in this case, the MVTP Client is an intermediate NDIS driver that provides a protocol interface to a WLAN (Wireless LAN) miniport driver. Therefore, a virtual PPP connection is created over a wireless LAN link to a MVTP FA. The MVTP Client WAN Miniport also receives and reponds to a set of WAN-specific OIDs passed to its MiniportQueryInformation and MiniportSetInformaion functions One of these OIDs, OID_WAN_SET_LINK_INFO, allows MaxSendFrameSize and MaxRecvFrameSize to be set.

RAS Components

Remote access components are a series of libraries that provide the Remote Access Service (RAS) programming interface for applications and PPP protocols (link control, authentication, and network control protocols). Remote access components can communicate directly with the NDISWAN driver or by accessing the Telephone API (TAPI). The remote access server instructs each WAN miniport driver (MVTP) to indicate when it goes into a line-up state. When the call is placed, the WAN miniport driver passes the line-up state indicator up through NDISWAN to the TAPI components. TAPI returns a call handle to NDISWAN to be used to refer to the physical connection, and then NDISWAN and the remote access components negotiate the rest of the remote access connection. PPP Authentication (PAP, CHAP) and network configuration protocols (IPCP, IPXCP, NBFCP, LCP, and so forth) are provided by the RAS system component. A WAN miniport driver implements only PPP media-specific framing

TAPI Components

TAPI components are a series of libraries that provide a call control programming interface for all TAPI-aware applications. TAPI components communicate directly with the NDISWAN driver to manage connections. The kernel-mode flow of communication is from NDISTAPI to NDISWAN, through NDIS to a TAPI-capable WAN miniport (MVTP). The NDISTAPI driver defines how WAN miniport drivers implement telephonic services. It is closely related to the Service Provider Interface established in Windows Telephony, with telephony-capable NDIS WAN miniport drivers providing kernel-mode support for user-mode TAPI service providers A TAPI-capable WAN miniport registers and initializes itself as a user of both WAN and TAPI services. When registration and initialization are complete, a user-level application can make telephonic requests to the user-mode KMDDSP service provider module which converts SPI requests to corresponding OIDs. The KMDDSP module passes the OIDs to the NDISTAPI driver, the kernel-mode component of TAPI. NDISTAPI routes the OIDs to the correct NDIS WAN miniport driver in order to set up, monitor, and tear down lines, and calls. NDISTAPI passes the OIDs in NdisRequest calls to the NDISWAN intermediate driver. NDISWAN passes these NDIS requests on, resulting in a call to the MiniportQueryInformation function or the MiniportSetInformation function of a TAPI-capable WAN miniport. A TAPI-capable WAN miniport communicates changes in the states of lines and calls, for instance a change from the proceeding state to the connected state, the arrival of an incoming call, or a remote disconnection. State changes are communicated to upper-layers by passing appropriate NDIS_STATUS_TAPI_*XXX* and NDIS_STATUS_WAN_*XXX* status messages to

NdisIndicateStatus. A WAN miniport calls **NdisMIndicateStatus** with a *GeneralStatus* value of NDIS_STATUS_WAN_LINE_UP to indicate that a new data channel has become active.

WLAN Miniport

The WLAN Miniport is a NDIS miniport NIC driver for an 802.11 Wireless LAN.

Appendix C – PPP/L2TP Source Code Vendors.

Telenetworks
6085 State Farm Drive
Rohnert Park, CA 94928
Voice: (707)584-6100
FAX: (707)584-6199
Contact: Bob Gefvert
www.telenetworks.com

Components:

SYS1001 (RTOS, device driver interface, System Management Entity) - $10,000
TNMP-100-001 (PPP/ML-PPP core) - $20,000
TNMP-102-001 (PAP/CHAP Authentication) - $5000
TNMP1101 (L2TP client and server) - $25,000

WindRiver
Contact: Terry Jobe
Voice: (612)837-6237
FAX: (612)837-6238
www.windriver.com

Routerware Components:

100-13743 (L2TP LAC & LNS) - $35,000
(PPP with all components) – approx. $100,000
100-13756 (RADIUS client extensions to PPP) - $20,000

United States Patent & Trademark Office

Office of Initial Patent Examination

Application papers not suitable for publication

SN 09729676 Mail Date 12-02-00

- ☐ Non-English Specification
- ☒ Specification contains drawing(s) on page(s) 7,8,9,10 or table(s)______
- ☐ Landscape orientation of text ☐ Specification ☐ Claims ☐ Abstract
- ☐ Handwritten ☐ Specification ☐ Claims ☐ Abstract
- ☐ More than one column ☐ Specification ☐ Claims ☐ Abstract
- ☒ Improper line spacing ☐ Specification ☐ Claims ☐ Abstract
- ☐ Claims not on separate page(s)
- ☐ Abstract not on separate page(s)
- ☐ Improper paper size -- Must be either A4 (21 cm x 29.7 cm) or 8-1/2"x 11"
  - ☐ Specification page(s)______ ☐ Abstract
  - ☐ Drawing page(s)______ ☐ Claim(s)
- ☐ Improper margins
  - ☐ Specification page(s)______ ☐ Abstract
  - ☐ Drawing page(s)______ ☐ Claim(s)
- ☐ Not reproducible

Reason	Section
☐ Paper too thin	☐ Specification page(s)______
☐ Glossy pages	☐ Drawing page(s)______
☐ Non-white background	☐ Abstract
	☐ Claim(s)

- ☐ Drawing objection(s)
  - ☐ Missing lead lines, drawing(s)______
  - ☐ Line quality is too light, drawing(s)______
  - ☐ More than 1 drawing and not numbered correctly
  - ☐ Non-English text, drawing(s)______
  - ☐ Excessive text, drawing(s)______
  - ☐ Photographs capable of illustration, drawing(s)______